DOCKET NO.: 266812US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takehiko NAKANO, et al.
SERIAL NO.: NEW U.S. PCT APPLICATION
FILED: HEREWITH
INTERNATIONAL APPLICATION NO.: PCT/JP04/09256
INTERNATIONAL FILING DATE: June 24, 2004
FOR: INFORMATION PROCESSING APPARATUS AND METHOD, RECORDING MEDIUM AND PROGRAM

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2003-281348	28 July 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/09256. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

PCT/JP2004/009256

日本国特許庁
JAPAN PATENT OFFICE

24.06.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　７月２８日

出願番号
Application Number: 特願２００３－２８１３４８

[ST. 10/C]: [ＪＰ２００３－２８１３４８]

出願人
Applicant(s): ソニー株式会社

２００４年　４月２８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０３７０９２

【書類名】　特許願
【整理番号】　0390540408
【提出日】　平成15年 7月28日
【あて先】　特許庁長官殿
【国際特許分類】　H04L　9/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　中野　雄彦
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082131
　【弁理士】
　【氏名又は名称】　稲本　義雄
　【電話番号】　03-3369-6479
【手数料の表示】
　【予納台帳番号】　032089
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9708842

【書類名】特許請求の範囲
【請求項１】
受信装置と共有する共有データを、前記受信装置に送信する共有データ送信手段と、
前記受信装置において前記共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信手段と、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づいて前記受信装置を認証する認証手段と、
前記受信装置からの、前記コマンドに対する応答時間を計測する計測手段と、
前記認証手段による認証結果、および前記計測手段により計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定手段と
を備えることを特徴とする情報処理装置。
【請求項２】
前記コマンド送信手段は、データの送信可否を判定するのに、前記コマンドを最大Ｎ回送信し、
前記認証手段は、前記コマンドの送信の順番に応じた前記認証データとその前記期待値とに基づいて、前記受信装置を認証する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項３】
受信装置と共有する共有データを、前記受信装置に送信する共有データ送信ステップと、
前記受信装置において前記共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づいて前記受信装置を認証する認証ステップと、
前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、
前記認証ステップでの認証結果、および前記計測ステップの処理で計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと
を含むことを特徴とする情報処理方法。
【請求項４】
受信装置と共有する共有データの、前記受信装置に対する送信を制御する共有データ送信制御ステップと、
前記受信装置において前記共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づく前記受信装置の認証を制御する認証制御ステップと、
前記受信装置からの、前記コマンドに対する応答時間の計測を制御する計測制御ステップと、
前記認証制御ステップでの認証結果、および前記計測制御ステップの処理で計測された応答時間に基づく、前記受信装置に対するデータの送信可否の判定を制御する判定制御ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項５】
受信装置と共有する共有データの、前記受信装置に対する送信を制御する共有データ送信制御ステップと、
前記受信装置において前記共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づく前記受信装置の認証を制御する認証制御ステップと、
前記受信装置からの、前記コマンドに対する応答時間の計測を制御する計測制御ステッ

プと、
　前記認証制御ステップでの認証結果、および前記計測制御ステップの処理で計測された応答時間に基づく、前記受信装置に対するデータの送信可否の判定を制御する判定制御ステップと
　を含む処理をコンピュータに実行させることを特徴とするプログラム。
【請求項６】
　送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置において、
　前記送信装置から前記コマンドが送信されてくる前に、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成手段と、
　前記送信装置から前記コマンドが送信されてくる前に、前記認証データ生成手段により生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成手段と、
　前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信手段と
　を備えることを特徴とする情報処理装置。
【請求項７】
　前記共有データは、疑似乱数であり、
　前記疑似乱数は、前記コマンドの前に前記送信装置から送信され、
　前記認証データ生成手段は、前記疑似乱数に対して鍵付きハッシュ処理を施し、その結果得られたハッシュ値を前記認証データとする
　ことを特徴とする請求項６に記載の情報処理装置。
【請求項８】
　前記認証データ生成手段は、前記疑似乱数と前記情報処理装置固有の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を前記認証データとする
　ことを特徴とする請求項７に記載の情報処理装置。
【請求項９】
　データの送信可否を判定するのに、前記送信装置から、前記コマンドが最大Ｎ回送信されてくる場合において、
　前記認証データ生成手段は、前記送信装置から最初の前記コマンドが送信されてくる前に、前記共有データに対して前記処理を施して、送信されてくるＮ個の前記コマンドのそれぞれに対応するＮ個の前記認証データを生成し、
　前記送信手段は、Ｎ個の前記認証データが、前記送信装置と予め合意した順番で前記送信装置に提供されるように、前記応答メッセージ生成手段により生成された前記応答メッセージを前記送信装置に送信する
　ことを特徴とする請求項６に記載の情報処理装置。
【請求項１０】
　前記認証データ生成手段は、前記共有データに対して前記処理を施して得られたデータを複数個に分割し、分割されたデータからＮ個の前記認証データを生成する
　ことを特徴とする請求項９に記載の情報処理装置。
【請求項１１】
　前記認証データ生成手段は、前記共有データに対して前記処理を繰り返し施し、その処理毎に得られたデータから、Ｎ個の前記認証データを生成する
　ことを特徴とする請求項９に記載の情報処理装置。
【請求項１２】
　前記送信手段は、前記送信装置からの前記コマンドが受信されたとき、前記認証データと前記コマンドに含まれる情報から生成された新たな認証データを含む応答メッセージを、前記送信装置に送信する
　ことを特徴とする請求項６に記載の情報処理装置。

【請求項１３】
送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置の情報処理方法において、
前記送信装置から前記コマンドが送信されてくる前に、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成ステップと、
前記送信装置から前記コマンドが送信されてくる前に、前記認証データ生成ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、
前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信ステップと
を含むことを特徴とする情報処理方法。
【請求項１４】
送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信するためのプログラムであって、
前記送信装置から前記コマンドが送信されてくる前の、前記共有データに対して所定の処理を施しての前記認証データの生成を制御する認証データ生成制御ステップと、
前記送信装置から前記コマンドが送信されてくる前の、前記認証データ生成制御ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、
前記送信装置から送信されてきた前記コマンドが受信されたときの、前記応答メッセージの前記送信装置に対する送信を制御する送信制御ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項１５】
送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信するためのプログラムであって、
前記送信装置から前記コマンドが送信されてくる前の、前記共有データに対して所定の処理を施しての前記認証データの生成を制御する認証データ生成制御ステップと、
前記送信装置から前記コマンドが送信されてくる前の、前記認証データ生成制御ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、
前記送信装置から送信されてきた前記コマンドが受信されたときの、前記応答メッセージの前記送信装置に対する送信を制御する送信制御ステップと
を含む処理をコンピュータに実行させることを特徴とするプログラム。

【書類名】明細書
【発明の名称】情報処理装置および方法、記録媒体、並びにプログラム
【技術分野】
【０００１】
本発明は、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、通信相手との通信時間を適切に計測することができるようにした情報処理装置および方法、記録媒体、並びにプログラムに関する。
【背景技術】
【０００２】
近年、インタネットに代表される公共性のある広域に亘るネットワーク（以下、WAN(Wide Area Network)と記述する）や一般家屋等に設けられる局所的なネットワーク（以下、ＬＡＮ(Local Area Network)と記述する）の普及に伴い、それらのネットワークを介した各種データ通信が盛んに行われている。その通信形態の１つのとして、通信相手との通信距離に応じて通信を制御することが提案されている。例えば、コンテンツの不正配布を防止するために、同一のＬＡＮに接続されている端末（通信距離が短い端末）間においてのみデータの授受が可能となるように通信が制御される。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
ところで、このように通信相手との通信距離に応じて通信を制御する場合、通信距離を判別する（同一のＬＡＮに接続されているか否かを判定する）必要があるが、従来では、送信側が所定の要求に対する受信側からの応答時間を計測し、計測したその応答時間に基づいて通信距離を判別する方法が存在しなかった。
【０００４】
本発明はこのような状況に鑑みてなされたものであり、応答時間を適切に計測し、その応答時間に基づいて通信距離を判別することを目的とする。
【課題を解決するための手段】
【０００５】
本発明の第１の情報処理装置は、受信装置と共有する共有データを、受信装置に送信する共有データ送信手段と、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信手段と、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証手段と、受信装置からの、コマンドに対する応答時間を計測する計測手段と、認証手段による認証結果、および計測手段により計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定手段とを備えることを特徴とする。
【０００６】
コマンド送信手段は、データの送信可否を判定するのに、コマンドを最大Ｎ回送信し、認証手段は、コマンドの送信の順番に応じた認証データとその期待値とに基づいて、受信装置を認証することができる。
【０００７】
本発明の第１の情報処理方法は、受信装置と共有する共有データを、受信装置に送信する共有データ送信ステップと、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップでの認証結果、および計測ステップの処理で計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップとを含むことを特徴とする。
【０００８】
本発明の第１の記録媒体のプログラムは、受信装置と共有する共有データの、受信装置

に対する送信を制御する共有データ送信制御ステップと、受信装置において共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づく受信装置の認証を制御する認証制御ステップと、受信装置からの、コマンドに対する応答時間の計測を制御する計測制御ステップと、認証制御ステップでの認証結果、および計測制御ステップの処理で計測された応答時間に基づく、受信装置に対するデータの送信可否の判定を制御する判定制御ステップとを含むことを特徴とする。

【０００９】

本発明の第１のプログラムは、受信装置と共有する共有データの、受信装置に対する送信を制御する共有データ送信制御ステップと、受信装置において共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づく受信装置の認証を制御する認証制御ステップと、受信装置からの、コマンドに対する応答時間の計測を制御する計測制御ステップと、認証制御ステップでの認証結果、および計測制御ステップの処理で計測された応答時間に基づく、受信装置に対するデータの送信可否の判定を制御する判定制御ステップとを含む処理をコンピュータに実行させることを特徴とする。

【００１０】

本発明の第１の情報処理装置および方法、並びにプログラムにおいては、受信装置と共有する共有データが、受信装置に送信され、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドが受信装置に送信され、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置が認証され、受信装置からの、コマンドに対する応答時間が計測され、認証結果、および応答時間に基づいて、受信装置に対するデータの送信可否が判定される。

【００１１】

本発明の第２の情報処理装置は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成手段と、送信装置からコマンドが送信されてくる前に、認証データ生成手段により生成された認証データを含む、コマンドに対する応答メッセージを生成する応答メッセージ生成手段と、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信手段とを備えることを特徴とする。

【００１２】

共有データは、疑似乱数であるようにし、疑似乱数は、コマンドの前に送信装置から送信されるようにし、認証データ生成手段は、疑似乱数に対して鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

【００１３】

認証データ生成手段は、疑似乱数と情報処理装置固有の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

【００１４】

データの送信可否を判定するのに、送信装置から、コマンドが最大Ｎ回送信されてくる場合において、認証データ生成手段は、送信装置から最初のコマンドが送信されてくる前に、共有データに対して処理を施して、送信されてくるＮ個のコマンドのそれぞれに対応するＮ個の認証データを生成し、送信手段は、Ｎ個の認証データが、送信装置と予め合意した順番で送信装置に提供されるように、応答メッセージ生成手段により生成された応答メッセージを送信装置に送信することができる。

【００１５】

認証データ生成手段は、共有データに対して処理を施して得られたデータを複数個に分割し、分割されたデータからＮ個の認証データを生成することができる。

【００１６】

認証データ生成手段は、共有データに対して処理を繰り返し施し、その処理毎に得られたデータから、Ｎ個の認証データを生成することができる。

【００１７】

送信手段は、送信装置からのコマンドが受信されたとき、認証データとコマンドに含まれる情報から生成された新たな認証データを含む応答メッセージを、記送信装置に送信することができる。

【００１８】

本発明の第２の情報処理方法は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成ステップと、送信装置からコマンドが送信されてくる前に、認証データ生成ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信ステップとを含むことを特徴とする。

【００１９】

本発明の第２の記録媒体のプログラムは、送信装置からコマンドが送信されてくる前の、共有データに対して所定の処理を施しての認証データの生成を制御する認証データ生成制御ステップと、送信装置からコマンドが送信されてくる前の、認証データ生成制御ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、送信装置から送信されてきたコマンドが受信されたときの、応答メッセージの送信装置に対する送信を制御する送信制御ステップとを含むことを特徴とする。

【００２０】

本発明の第２のプログラムは、送信装置からコマンドが送信されてくる前の、共有データに対して所定の処理を施しての認証データの生成を制御する認証データ生成制御ステップと、送信装置からコマンドが送信されてくる前の、認証データ生成制御ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、送信装置から送信されてきたコマンドが受信されたときの、応答メッセージの送信装置に対する送信を制御する送信制御ステップとを含むことを特徴とする。

【発明の効果】

【００２１】

第１の本発明によれば、受信装置の応答時間を適切に計測することができる。

【００２２】

第２の本発明によれば、送信装置における応答時間の適切な計測に必要な情報を提供することができる。

【発明を実施するための最良の形態】

【００２３】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００２４】

本発明の第１の情報処理装置は、受信装置と共有する共有データ（例えば、ランダムチャレンジ）を、受信装置に送信する共有データ送信手段（例えば、図３のランダムチャレンジ送信制御部３２）と、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信手段（例えば、図３のコマンド送信制御部３４）と、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証手段（例えば、図３の判定部３５）と、受信装置からの、コマンドに対する応答時間を計測する計測手段（例えば、図３の応答時間計測部３６）と、認証手段による認証結果、および計測手段により計測さ

れた応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定手段（例えば、図３の判定部３５）とを備えることを特徴とする。

【００２５】

コマンド送信手段は、データの送信可否を判定するのに、コマンドを最大Ｎ回送信し（例えば、図５のステップＳ６，１２，１３）、認証手段は、コマンドの送信の順番に応じた認証データとその期待値とに基づいて、受信装置を認証することができる（例えば、図５のステップＳ１０）。

【００２６】

本発明の第１の情報処理方法は、受信装置と共有する共有データを、受信装置に送信する共有データ送信ステップ（例えば、図５のステップＳ２）と、受信装置において共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信ステップ（例えば、図５のステップＳ６）と、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証ステップ（例えば、図５のステップＳ１０）と、受信装置からの、コマンドに対する応答時間を計測する計測ステップ（例えば、図５のステップＳ７，Ｓ９）と、認証ステップでの認証結果、および計測ステップの処理で計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップ（例えば、図５のステップＳ１１，Ｓ１４，Ｓ１５）とを含むことを特徴とする。

【００２７】

本発明の第２の情報処理装置は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成手段（例えば、図４の認証データ生成部４２）と、送信装置からコマンドが送信されてくる前に、認証データ生成手段により生成された認証データを含む、コマンドに対する応答メッセージを生成する応答メッセージ生成手段（例えば、図４の応答メッセージ生成部４３）と、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信手段（例えば、応答メッセージ送信制御部４４）とを備えることを特徴とする。

【００２８】

共有データは、疑似乱数（例えば、ランダムチャレンジ）であるようにし、疑似乱数は、コマンドの前に送信装置から送信されるようにし（例えば、図５のステップＳ２）、認証データ生成手段は、疑似乱数に対して鍵付きハッシュ処理（例えば、ＨＭＡＣ（RFC 2104）アルゴリズムによるハッシュ処理）を施し、その結果得られたハッシュ値を認証データとすることができる。

【００２９】

認証データ生成手段は、疑似乱数と情報処理装置固有（例えば、端末１１の機器ＩＤ）の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

【００３０】

データの送信可否を判定するのに、送信装置から、コマンドが最大Ｎ回送信されてくる場合において、認証データ生成手段は、送信装置から最初のコマンドが送信されてくる前に、共有データに対して処理を施して、送信されてくるＮ個のコマンドのそれぞれに対応するＮ個の認証データを生成し（例えば、図５のステップＳ２２）、送信手段は、Ｎ個の認証データが、送信装置と予め合意した順番で送信装置に提供されるように、応答メッセージ生成手段により生成された応答メッセージを送信装置に送信することができる（例えば、図５のステップＳ２７）。

【００３１】

認証データ生成手段は、共有データに対して処理を施して得られたデータを複数個に分割し、分割されたデータからＮ個の認証データ（例えば、図６に示す期待値と同様に生成された認証データ）を生成することができる。

【００３２】

認証データ生成手段は、共有データに対して処理を繰り返し施し、その処理毎に得られ

たデータから、N個の認証データ（例えば、図７に示す期待値と同様に生成された認証データ）を生成することができる。

【００３３】

送信手段は、送信装置からのコマンドが受信されたとき、認証データとコマンドに含まれる情報から生成された新たな認証データを含む応答メッセージを、記送信装置に送信することができる（例えば、図５のステップＳ２７）。

【００３４】

本発明の第２の情報処理方法は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成ステップと（例えば、図５のステップＳ２２）、送信装置からコマンドが送信されてくる前に、認証データ生成ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージを生成する応答メッセージ生成ステップ（例えば、図５のステップＳ２５）と、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信ステップ（例えば、図５のステップＳ２７）とを含むことを特徴とする。

【００３５】

図１は、本発明を適用した端末１１からなる情報通信システムの構成例を示している。

【００３６】

ＬＡＮ１－１，１－２（以下、個々に区別する必要がない場合、単位、ＬＡＮ１と称する。他の場合についても同様である）がインタネットに代表されるWAN２を介して相互に接続されている。

【００３７】

ＬＡＮ１－１は、例えば、家屋内に設けられ、特定の個人（あるいは、家族）が使用する程度の規模のものであり、それには、スイッチングハブ（図示せず）を介して、パーソナルコンピュータやＡＶ機器等の端末１１－１および端末１１－２が接続されている。ＬＡＮ１－１と端末１１－１および１１－２との接続は、例えば、Ethernet(R)（100BASE-TX）等の高速インタフェースによる。端末１１－１および１１－２は、ＬＡＮ１－１およびWAN２を介して、ＬＡＮ１－２に接続することができる。

【００３８】

ＬＡＮ１－２は、ＬＡＮ１－１と同様に構成されており、それには、端末１１－３が接続されている。

【００３９】

各端末１１は、本情報通信システムに登録された正規の機器であり、図２に示すように、送信可否判定部２１、応答制御部２２、通信部２３、および送信データ格納部２４を含んで構成されている。

【００４０】

送信可否判定部２１は、他の端末１１（受信側の端末１１）に所定のデータを送信する際に、通信部２３を介して、受信側の端末１１（正確には、その応答制御部２２）と後述するように通信することで、受信側の端末１１が本情報通信システムにおける正規の機器であるか否かを認証するとともに、所定の要求に対する受信側の端末１１の応答時間を、受信側の端末１１との通信時間として計測する。

【００４１】

送信可否判定部２１は、受信側の端末１１の認証結果および応答時間に基づく通信距離の判別結果に基づいて、受信側の端末１１に対するデータの送信可否を判定する。

【００４２】

例えば、受信側の端末１１が、送信側の端末１１と異なるＬＡＮ１に接続されている場合（ＷＡＮ２を介して接続され、いわゆる通信距離が長い場合）、応答時間は、同じＬＡＮ１に接続されている場合（通信距離が短い場合）に比べて長くなるので、例えば、通信が同一ＬＡＮ１内に制限されているとき、送信可否判定部２１は、計測した応答時間から受信側の端末１１が送信側の端末１１と同じＬＡＮ１に接続されているか否かを判定し、その判定結果と受信側の端末１１の認証結果に基づいて、データ送信の可否を判定する。

【００４３】
すなわち図１の例では、端末１１－１（送信側）が端末１１－２（受信側）にデータを送信する場合、端末１１－１の送信可否判定部２１は、計測した端末１１－２の応答時間から、端末１１－２がＬＡＮ１－１に接続されていることを判定し、データ送信を行う。一方、端末１１－１が端末１１－３にデータを送信する場合、端末１１－１の送信可否判定部２１は、計測した端末１１－３の応答時間から、端末１１－３はＬＡＮ１－１と異なるＬＡＮ（ＬＡＮ１－２）に接続されていることを判定し、データ送信を行わない。
【００４４】
なおこのような通信距離による通信制御は、映画などのコンテンツを一定の地域に対して先行配給し、他の地域には後日配給するなどのコンテンツ配給ビジネスに適用することができる。
【００４５】
図２に戻り、応答制御部２２は、送信側の端末１１から所定のデータの送信を受ける際、通信部２３を介して、送信側の端末１１（正確には、その送信可否判定部２１）と後述するように通信することで、送信側の端末１１における認証および応答時間の適切な計測に必要な情報を送信側の端末１１に送信する。
【００４６】
通信部２３は、ＬＡＮ１に接続されており、同一のＬＡＮ１内の端末１１、またはＷＡＮ２を介して異なるＬＡＮ１に接続されている端末１１との通信を行う。
【００４７】
送信データ格納部２４は、受信側の端末１１に送信される、所定のデータが格納されている。
【００４８】
図３は、端末１１の送信可否判定部２１の構成例を示している。
【００４９】
ランダムチャレンジ生成部３１は、所定ビット数の疑似乱数（以下、ランダムチャレンジと称する）を生成し、ランダムチャレンジ送信制御部３２および期待値生成部３３に供給する。
【００５０】
ランダムチャレンジ送信制御部３２は、ランダムチャレンジ生成部３１から供給されたランダムチャレンジを、通信部２３を介して、受信側の端末１１に送信する。ランダムチャレンジ送信制御部３２はまた、通信部２３を介して、受信側の端末１１から送信されてきた、ランダムチャレンジを受信した旨のメッセージ（以下、ＲＣ受信メッセージと称する）を受信し、そのときＲＣ受信メッセージを受信した旨をコマンド送信制御部３４に通知する。
【００５１】
期待値生成部３３は、ランダムチャレンジ生成部３１から供給されたランダムチャレンジに対して、例えば、受信側の端末１１と共有する秘密鍵を利用したＨＭＡＣ（RFC 2104）アルゴリズムによるハッシュ処理（いわゆる鍵付きハッシュ処理）を施して、受信側の端末１１でランダムチャレンジから生成される認証データの期待値を生成し、判定部３５に供給する。期待値生成部３３はまた、端末１１に予め設定された端末１１固有の情報（例えば、機器ＩＤ）とランダムチャレンジを連結したものに鍵付きハッシュ処理を施して期待値を生成することもできる。
【００５２】
なお、ハッシュ処理で利用される秘密鍵は、本情報通信システムの正規の機器に所定のタイミングで安全に配信される。
【００５３】
コマンド送信制御部３４は、ランダム送信制御部３２から、ＲＣ受信メッセージを受信した旨が通知されたとき、または判定部３５からの指示に従って、応答を要求するコマンド（以下、応答要求コマンドと称する）を、通信部２３を介して、受信側の端末１１に送

信する。

【００５４】

コマンド送信制御部３４または、通信部２３を介して、送信した応答要求コマンドに対する応答として、受信側の端末１１から送信されてきたメッセージ（以下、応答メッセージと称する）を受信し、それを判定部３５に供給する。応答メッセージには、ランダムチャレンジ送信制御部３２により送信されたランダムチャレンジから生成された認証データが組み込まれている。

【００５５】

コマンド送信制御部３４または、応答要求コマンドを送信した後、応答時間計測部３６を制御して、応答時間の計測を開始させるとともに、その応答要求コマンドに対する応答としての応答メッセージを受信したとき、応答時間の計測を終了させる。

【００５６】

判定部３５は、コマンド送信制御部３４からの応答メッセージに組み込まれている認証データと、期待値生成部３３で生成されたその認証データの期待値に基づいて、受信側の端末１１が、本情報通信システムにおける正規の機器であるかの認証を行う。判定部３５はまた、応答時間計測部３６で計測された応答時間が所定の時間Ｘを越えているか否かを判定して、通信距離の判別（送信側の端末１１と同一のＬＡＮ１に接続されているかの判定）を行う。

【００５７】

判定部３５は、受信側の端末１１の認証結果および通信距離の判別結果に基づいて、データの送信可否の判定を行う。判定部３５は、その判定結果に基づいて、通信部２３を制御し、送信データ格納部２４に格納されているデータを、受信側の端末１１に送信させる。

【００５８】

応答時間計測部３６は、コマンド送信制御部３４からの指示に従って、内蔵するタイマを動作させ、受信側の端末１１の応答時間を計測する。

【００５９】

図４は、端末１１の応答制御部２２の構成例を示している。

【００６０】

ランダムチャレンジ受信制御部４１は、通信部２３を介して、送信側の端末１１（正確には、その送信可否判定部２１）から送信されてきたランダムチャレンジを受信し、それを認証データ生成部４２に供給する。ランダムチャレンジ受信制御部４１はまた、通信部２３を介して、ＲＣ受信メッセージ（ランダムチャレンジを受信した旨を表すメッセージ）を、送信側の端末１１に送信し、そのときＲＣ受信メッセージを送信した旨を応答メッセージ送信制御部４４に通知する。

【００６１】

認証データ生成部４２は、ランダムチャレンジ受信制御部４１から供給されたランダムチャレンジに対して、送信側の端末１１（送信可否判定部２１の期待値生成部３３）における場合と同様の鍵付きハッシュ処理を施して、第三者が予測できない認証データを生成し、応答メッセージ生成部４３に供給する。

【００６２】

応答メッセージ生成部４３は、応答メッセージ送信制御部４４の制御に従って、認証データ生成部４２から供給された認証データを組み込んだ応答メッセージを生成し、応答メッセージ送信制御部４４に供給する。

【００６３】

応答メッセージ送信制御部４４は、通信部２３を介して、送信側の端末１１から送信されてきた応答要求コマンドを受信する。

【００６４】

応答メッセージ送信制御部４４は、応答要求コマンドを受信する前のタイミングで（送信側の端末１１から応答要求コマンドが送信されてくる前のタイミングで）、応答メッセ

ージ生成部４３を制御して、受信する応答要求コマンドに対応した認証データが組み込まれた応答メッセージを生成させるとともに、応答要求コマンドを受信したとき、通信部２３を介して、その応答メッセージを送信先の端末１１に送信する。

【００６５】

次に、図５のフローチャートを参照して、送信可否判定処理を行う場合の端末１１の送信可否判定部２１（図２，３）の動作を説明する。

【００６６】

ステップＳ１において、端末１１（送信側の端末１１）の送信可否判定部２１のランダムチャレンジ生成部３１は、ランダムチャレンジを生成し、それをランダムチャレンジ送信制御部３２および期待値生成部３３に供給する。

【００６７】

ステップＳ２において、ランダムチャレンジ送信制御部３２は、供給されたランダムチャレンジを、通信部２３を介して受信側の端末１１に送信し、ステップＳ３において、期待値生成部３３は、供給されたランダムチャレンジに対して鍵付きハッシュ処理を施して、受信側の端末１１で生成される認証データの期待値を生成する。

【００６８】

なおこの例の場合、送信側の端末１１は、データ送信の可否を判定するのに、最大Ｎ（＝１，２，・・・）回応答要求コマンドを送信するので、ここでは、送信され得るＮ個の応答要求コマンドに応じた認証データのＮ個の期待値が生成される。

【００６９】

Ｎ個の期待値は、例えば、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータを複数個に分割し、その分割して得られたデータからＮ個の期待値を生成することができる。図６の例の場合、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータが、Ｎ個に分割されて、Ｎ個の期待値１乃至期待値Ｎが生成される。

【００７０】

また、ランダムチャレンジに対する鍵付きハッシュ処理を、複数回繰り返して行い、その処理毎に得られたデータから、Ｎ個の期待値を生成することができる。図７の例の場合、ランダムチャレンジに対する鍵付きハッシュ処理がＮ回繰り返して行われ、その処理毎に得られたＮ個のデータが期待値となる。図７中、期待値１は、ランダムチャレンジに鍵付きハッシュ処理が１回施された結果得られたものであり、期待値２は、期待値１に、鍵付きハッシュ処理がさらに施された結果得られたものである。

【００７１】

図５に戻り、ステップＳ４において、ランダムチャレンジ送信制御部３２は、後述するように受信側の端末１１から送信されてきた、ステップＳ２で送信されたランダムチャレンジを受信した旨を示すＲＣ受信メッセージを（ステップＳ２３）、通信部２３を介して受信し、その旨をコマンド送信制御部３４に通知する。ステップＳ５において、コマンド送信制御部３４は、応答要求コマンドが何番目に送信されるものか（送信の順番）を示すカウンタｉに１を初期設定する。

【００７２】

次に、ステップＳ６において、コマンド送信制御部３４は、通信部２３を介して、応答要求コマンドを受信側の端末１１に送信し、ステップＳ７において、応答時間計測部３６を制御して、応答時間の計測を開始させる。

【００７３】

ステップＳ８において、コマンド送信制御部３４は、後述するように受信側の端末１１から送信されてきた、ステップＳ６で送信された応答要求コマンドに対する応答しての応答メッセージを、通信部２３を介して受信して、判定部３５に供給し、ステップＳ９において、応答時間計測部３６を制御して、応答時間の計測を終了させる。すなわちステップＳ７で開始しステップＳ９で終了する時間計測で得られた時間が受信側の端末１１の応答時間となる。

【００７４】
ステップＳ１０において、判定部３５は、コマンド送信制御部３４から供給された応答メッセージに組み込まれている認証データと、期待値生成部３３により生成された、その認証データの期待値（具体的には、カウンタｉが示す順番に送信された応答要求コマンド（以下、第ｉ番目に送信された応答要求コマンドと称する）に対応する期待値）とが一致するか否かを判定し、一致すると判定した場合、受信側の端末１１を、情報通信システムにおける正規の端末であると認証し、ステップＳ１１に進む。
【００７５】
ステップＳ１１において、判定部３５は、応答時間計測部３で計測された、第ｉ番目に送信された応答要求コマンドに対する受信側の端末１１の応答時間が所定の時間Ｘを越えているか否かを判定する。時間Ｘは、例えば、同一ＬＡＮ１に接続された端末１１間で要する通信時間である。すなわち応答時間が時間Ｘを越える場合、受信側の端末１１は、送信側の端末１１と異なるＬＡＮ１に接続され、また、時間Ｘを越えない場合（応答時間＝時間Ｘを含む）、同一のＬＡＮ１に接続されていると判定することができる（通信距離を判別することができる）。
【００７６】
ステップＳ１１で、時間Ｘを越えると判定された場合、ステップＳ１２に進み、判定部３５は、その結果を、コマンド送信制御部３４に通知し、コマンド送信制御部３４はそのとき、カウンタｉを１だけインクリメントする。
【００７７】
ステップＳ１３において、コマンド送信制御部３４は、カウンタｉ＝Ｎ＋１であるか否かを判定する。ステップＳ１３で、カウンタｉ＝Ｎ＋１であると判定されたとき（すなわち、応答要求コマンドの送信がＮ回行われたとき）、またはステップＳ１０で、受信側の端末１１が本情報通信システムにおける正規の機器ではないと判定されたとき、ステップＳ１４に進み、その旨を、判定部３５に通知する。判定部３５はそのとき、受信側の端末１１へのデータ送信を不可とし、通信部２３を制御して、送信データ格納部２４に格納されているデータの受信側の端末１１に対する送信を禁止する。
【００７８】
ステップＳ１１で、第ｉ番目に送信された応答要求コマンドに対する応答時間が、時間Ｘを越えないと判定された場合、すなわち、受信側の端末１１が、本情報通信システムにおける正規の機器であり、かつ、例えば送信側の端末１１と同じＬＡＮ１に接続されている端末１１であるとき、ステップＳ１５に進み、判定部３５は、通信部２３を制御して、送信データ格納部２４に格納されているデータを、受信側の端末１１に送信させる。
【００７９】
ステップＳ１４またはステップＳ１５で、受信側の端末１１に対するデータ送信可否が判定されたとき、判定部３５は、通信部２３を介して、送信可否判定が終了した旨を表すメッセージ（以下、判定終了メッセージと称する）を受信側の端末１１に送信する。その後、送信可否判定処理は、処理を終了する。
【００８０】
次に、図５のフローチャートを参照して、応答処理を行う場合の端末１１の応答制御部２２（図２，４）の動作を説明する。
【００８１】
ステップＳ２１において、端末１１（受信側の端末１１）の応答制御部２２のランダムチャレンジ受信制御部４１は、送信先の端末１１から送信されてきたランダムチャレンジを（ステップＳ２）、通信部２３を介して受信し、認証データ生成部４２に供給する。ステップＳ２２において、認証データ生成部４２は、ランダムチャレンジ受信制御部４１から供給されたランダムチャレンジに対して、送信側の端末１１の送信可否判定部２１（期待値生成部３３）における鍵付きハッシュ処理（ステップＳ３）と同様の鍵付きハッシュ処理を施し、認証データを生成し、応答メッセージ生成部４３に供給する。
【００８２】

なおこの例では、最大Ｎ個の応答要求コマンドを受信し得るので、その応答要求コマンドに対応する期待値と対比される（ステップＳ１０）Ｎ個の認証データが生成される。Ｎ個の認証データは、期待値の生成方法（図６，７）と同じ方法で生成される。

【００８３】

このように認証データが生成されると、ステップＳ２３において、ランダムチャレンジ受信制御部４１は、通信部２３を介して、ＲＣ受信メッセージを送信側の端末１１に送信し、その旨を、応答メッセージ送信制御部４４に通知する。

【００８４】

ステップＳ２４において、応答メッセージ送信制御部４４は、これから受信する応答要求コマンドが何番目に受信されるものかを示すカウンタｊに１を初期設定し、ステップＳ２５において、応答メッセージ生成部４３を制御して、カウンタｊが示す順番に受信される応答要求コマンド（以下、第ｊ番目に受信される応答要求コマンドと称する）に対応する認証データを組み込んだ応答メッセージを生成させる。

【００８５】

次に、ステップＳ２６において、応答メッセージ送信制御部４４は、送信先の端末１１から送信されてきた応答要求コマンドを（ステップＳ６）、通信部２３を介して受信すると、ステップＳ２７において、ステップＳ２５で生成された第ｊ番目に受信される応答要求コマンドに応じた認証データが組み込まれた応答メッセージを、通信部２３を介して、送信側の端末１１に送信する。これにより上述したように送信側の端末１１で（ステップＳ１０で）、第ｊ番目に受信された（第ｉ番目に送信された）応答要求コマンドに対応する認証データと、第ｉ番目に送信された（第ｊ番目に受信された）応答要求コマンドの期待値とが比較される。

【００８６】

ステップＳ２８において、受信側の端末１１の応答制御部２２の応答メッセージ送信制御部４４は、送信側の端末１１から送信される判定終了メッセージ（ステップＳ１６）が受信されたか否かを判定し、受信されていないと判定した場合、ステップＳ２９に進む。ステップＳ２９において、応答メッセージ送信制御部４４は、カウンタｊを１だけインクリメントし、ステップＳ３０で、カウンタｊ＝Ｎ＋１であるか否かを判定する。

【００８７】

ステップＳ３０で、カウンタｊ＝ｊ＋１ではないと判定されたとき（すなわち、応答要求コマンドをＮ回受信されていないとき）、ステップＳ２５に戻り、次に受信される応答要求コマンドに対して、それ以降の処理を実行する。

【００８８】

ステップＳ２８で、判定終了メッセージが受信されたとき、またはステップＳ３０で、カウンタｊ＝Ｎ＋１であると判定されたとき（すなわち、応答要求コマンドがＮ回受信されたとき）、応答制御部２２は、応答処理を終了する。

【００８９】

以上のように、ランダムチャレンジから生成された認証データ（ステップＳ２２）とその期待値（ステップＳ３）とに基づいて認証された受信側の端末１１についてのみ応答時間に基づく通信距離の判別を行うようにしたので（ステップＳ１０でＮＯの判定がなされた場合、ステップＳ１１の処理がスキップされるので）、正規の機器のようになりすました機器にデータが送信されることを防止することができる（正規の機器のようになりすました機器が応答要求コマンドを受信し、応答要求メッセージを送信して、その機器にデータが送信されることはない）。

【００９０】

また送信側の端末１１で、応答要求コマンドに、新たに生成したランダムチャレンジを込み込んで受信側の端末１１に送信し（ステップＳ６）、受信側の端末１１で、応答要求コマンドを受信したとき（ステップＳ２６）、予め生成された認証データ（ステップＳ２２）と、その応答要求コマンドに組み込まれたランダムチャレンジとを連結して、または両者の論理演算を行って新たな認証データを生成し、それを組み込んだ応答メッセージを

返信することもできる（ステップＳ２７）。なお送信側の端末１１では、ステップＳ１０で新たな認証データと比較される期待値が、ステップＳ３で生成された期待値と、応答要求コマンドに組み込まれたランダムチャレンジと連結されて、または両者の論理演算が行われて生成される。

【００９１】

このように応答要求コマンドに組み込んだランダムチャレンジを利用して認証データおよび期待値が生成されるようにすることで、受信側の端末１１は、送信側の端末１１からの応答要求コマンドを受信した後でなければ、応答メッセージを送信することができなくなる。したがって、応答時間を短縮するために、応答要求コマンドを受信する前に応答メッセージを送信するなどといった不正行為を防止することができる。

【００９２】

また、以上のように、受信側の端末１１において、応答要求コマンドを受信する前に、認証データおよびそれが組み込まれた応答メッセージを生成するようにしたので（ステップＳ２２，Ｓ２５）、応答要求コマンドを受信した後直ちに応答メッセージを送信側の端末１１に返信することができる（ステップＳ２７）。

【００９３】

例えば、応答要求コマンドを受信した後に、認証データおよび応答要求メッセージを生成するようになされている場合、送信側の端末１１で計測される応答時間に、その処理にかかる時間が含まれてしまうので、通信時間としての応答時間を正確に計測することができない。しかしながら本発明のように応答要求コマンドを受信した後直ちに応答メッセージを送信することができるようにしておくことにより、通信時間としての応答時間を正確に計測することができる。

【００９４】

上述した一連の処理は、ハードウエアにより実現させることもできるが、ソフトウエアにより実現させることもできる。一連の処理をソフトウエアにより実現する場合には、そのソフトウエアを構成するプログラムがコンピュータにインストールされ、そのプログラムがコンピュータで実行されることより、上述した送信可否判定部２１および応答制御部２２が機能的に実現される。

【００９５】

図８は、上述のような送信可否判定部２１および応答制御部２２として機能するコンピュータ１０１の一実施の形態の構成を示すブロック図である。CPU（Central Processing Unit）１１１にはバス１１５を介して入出力インタフェース１１６が接続されており、CPU１１１は、入出力インタフェース１１６を介して、ユーザから、キーボード、マウスなどよりなる入力部１１７から指令が入力されると、例えば、ROM（Read Only Memory）１１２、ハードディスク１１４、またはドライブ１２０に装着される磁気ディスク１３１、光ディスク１３２、光磁気ディスク１３３、若しくは半導体メモリ１３４などの記録媒体に格納されているプログラムを、RAM（Random Access Memory）１１３にロードして実行する。これにより、上述した各種の処理（例えば、図５のフローチャートにより示される処理）が行われる。さらに、CPU１１１は、その処理結果を、例えば、入出力インタフェース１１６を介して、LCD（Liquid Crystal Display）などよりなる出力部１１８に必要に応じて出力する。なお、プログラムは、ハードディスク１１４やROM１１２に予め記憶しておき、コンピュータ１０１と一体的にユーザに提供したり、磁気ディスク１３１、光ディスク１３２、光磁気ディスク１３３，半導体メモリ１３４等のパッケージメディアとして提供したり、衛星、ネットワーク等から通信部１１９を介してハードディスク１１４に提供することができる。

【００９６】

なお、本明細書において、記録媒体により提供されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【００９７】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【図面の簡単な説明】

【００９８】

【図１】本発明を適用した情報通信システムの利用例を示す図である。

【図２】図１の端末の構成例を示すブロック図である。

【図３】図２の送信可否判定部の構成例を示すブロック図である。

【図４】図２の応答制御部の構成例を示すブロック図である。

【図５】送信可否判定処理および応答処理を説明するフローチャートである。

【図６】期待値および認証データの生成方法を説明する図である。

【図７】期待値および認証データの他の生成方法を説明する図である。

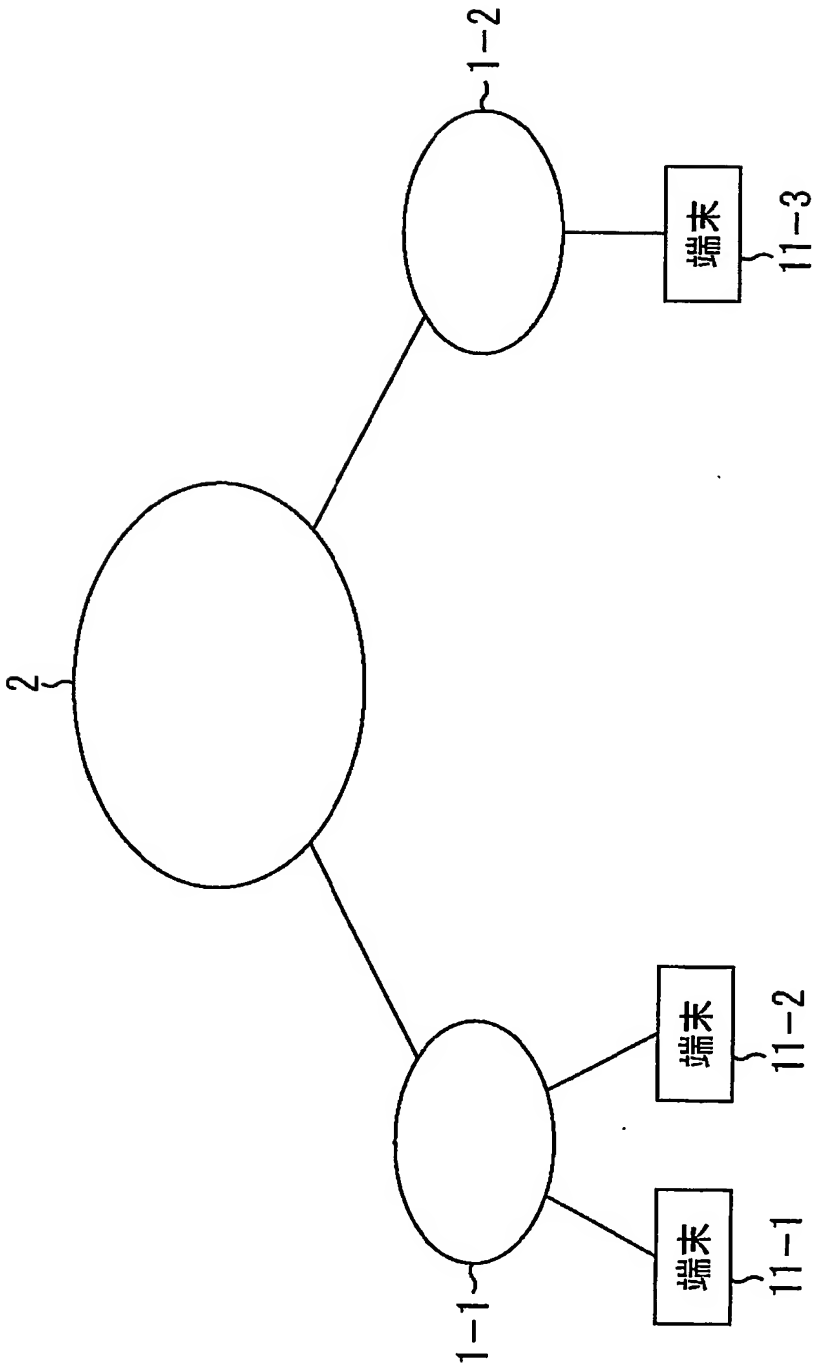
【図８】パーソナルコンピュータの構成例を示すブロック図である。

【符号の説明】

【００９９】

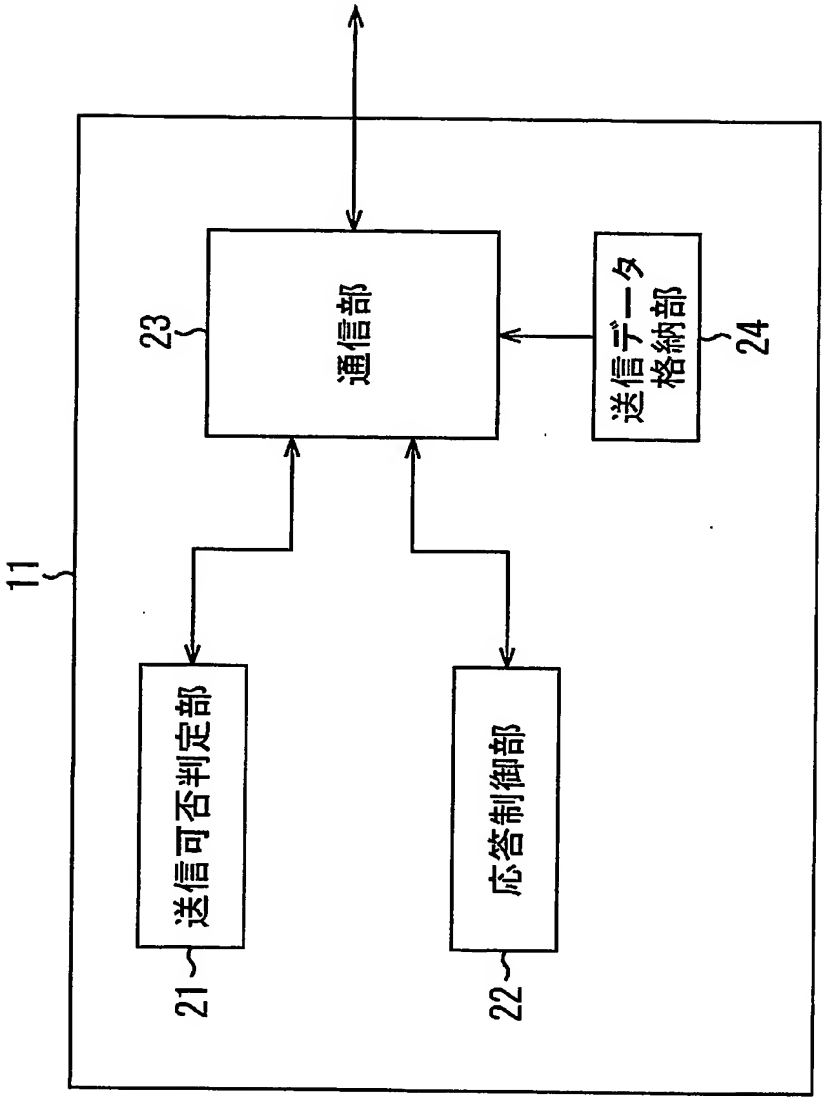
１　ＬＡＮ，　２　ＷＡＮ，　１１　端末，　２１　送信可否探偵部，　２２　応答制御部，　２３　通信部２３，　２４　送信データ格納部，　３１　ランダムチャレンジ生成部，　３２　ランダムチャレンジ送信制御部，　３３　期待値生成部，　３４　コマンド送信制御部，　３５　判定部，　３６　応答時間計測部

【書類名】図面
【図１】
図1



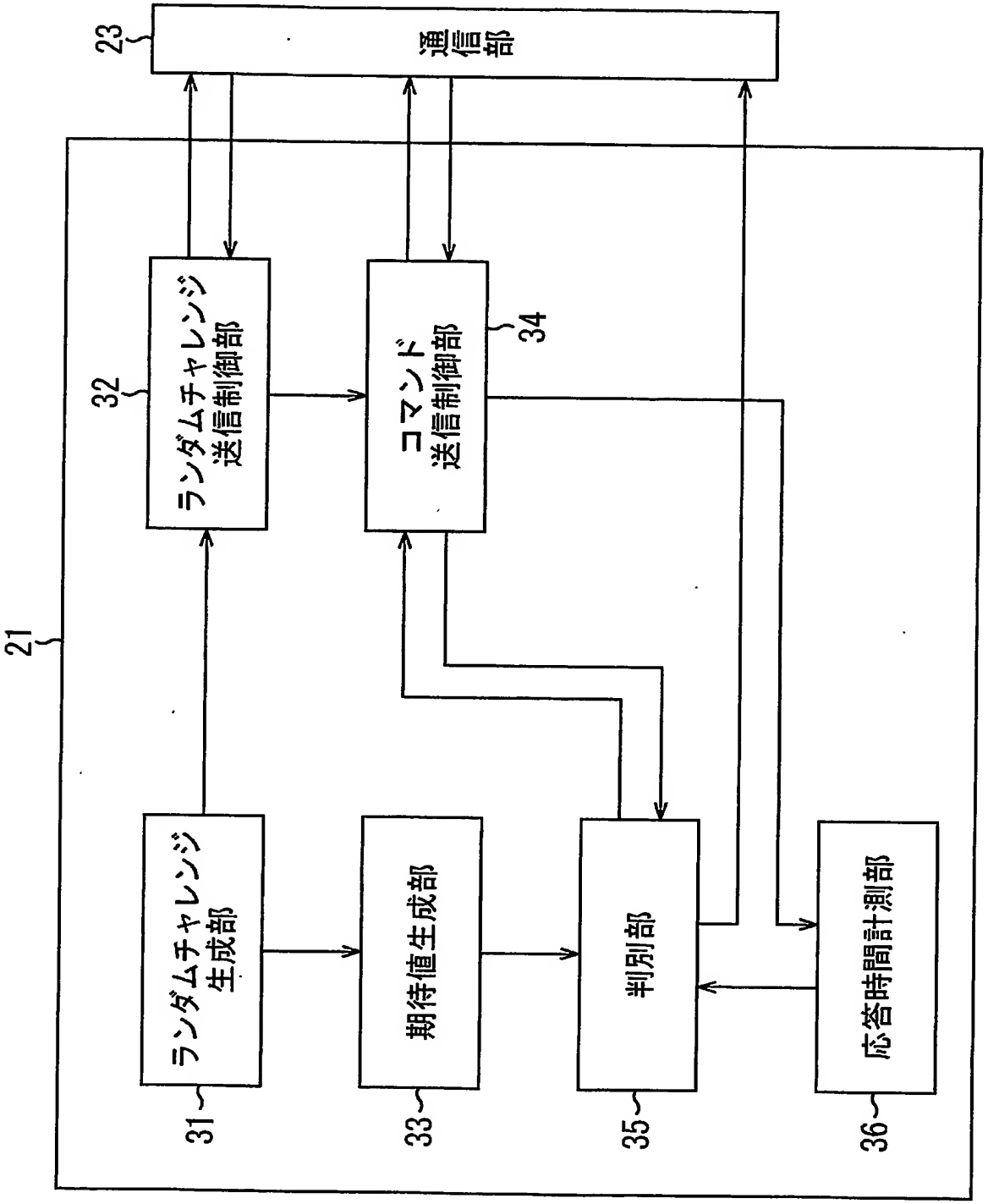
【図２】

図2



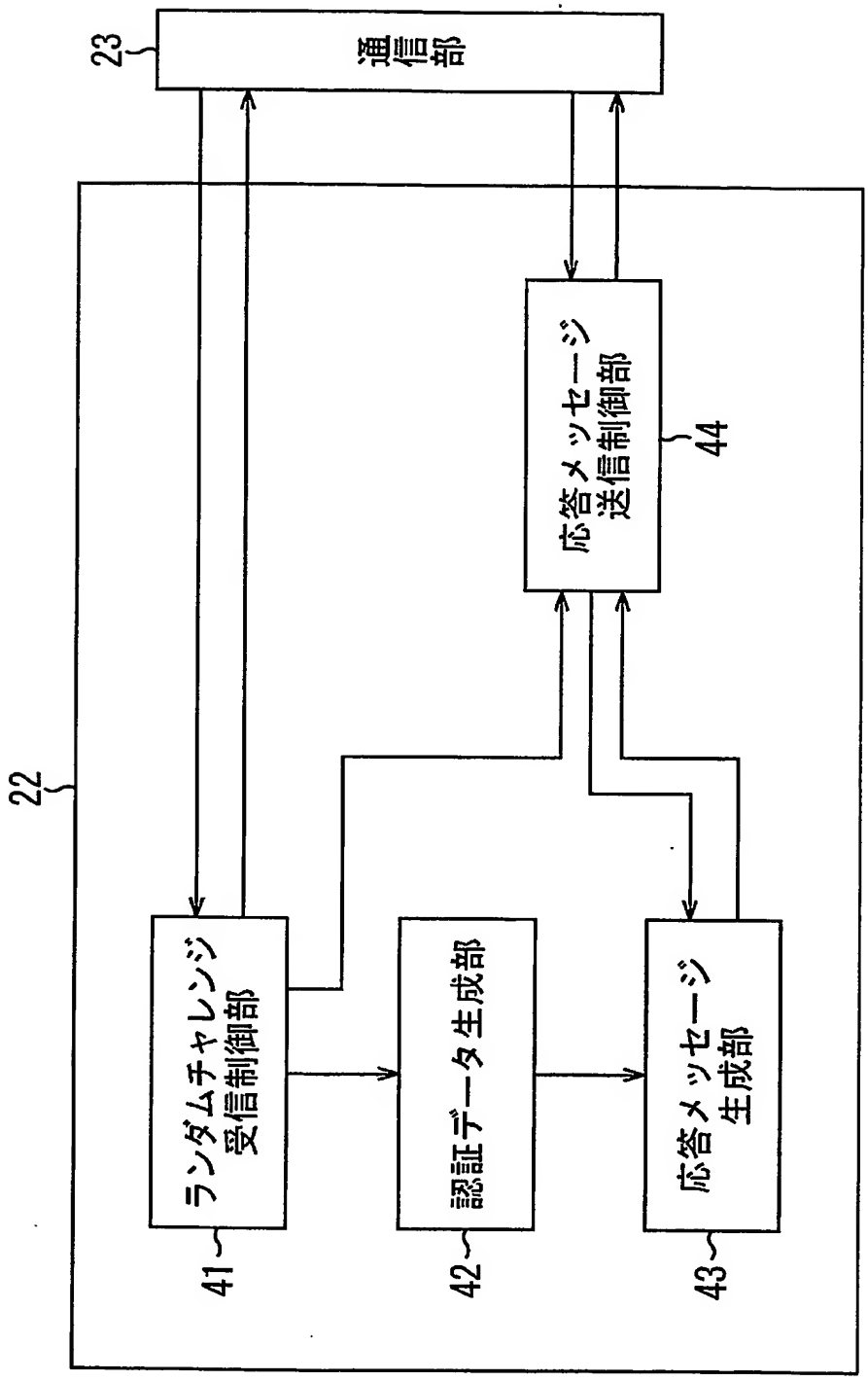
【図３】

図3


23
通信部
21
32
ランダムチャレンジ送信制御部
34
コマンド送信制御部
ランダムチャレンジ生成部
31
期待値生成部
33
判別部
35
応答時間計測部
36

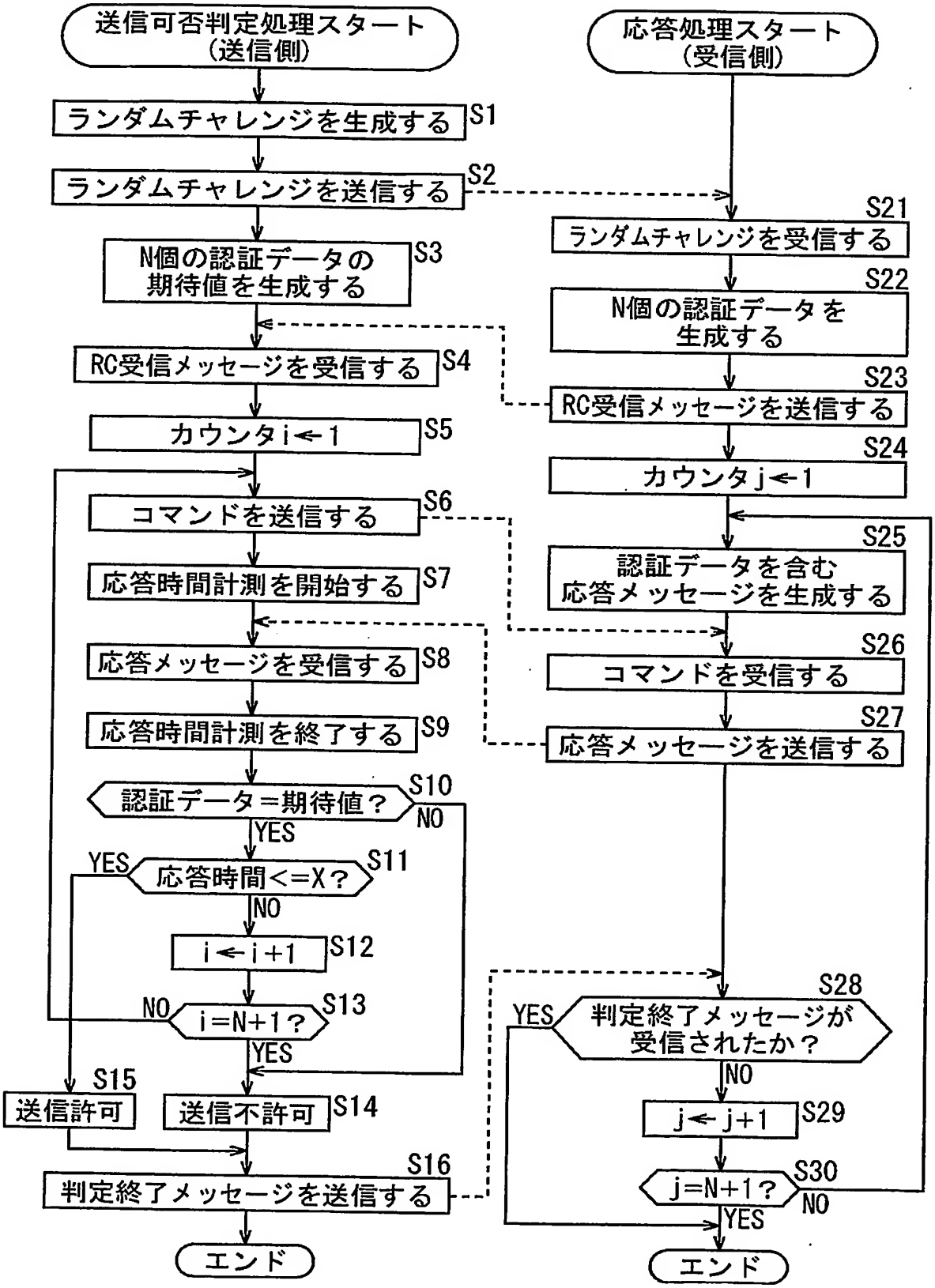
【図４】

図4


23
通信部
22
応答メッセージ
送信制御部
44
ランダムチャレンジ
受信制御部
41
認証データ生成部
42
応答メッセージ
生成部
43

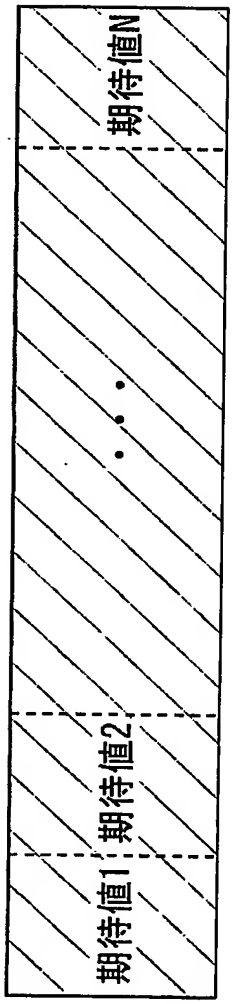
【図５】

図5


送信可否判定処理スタート
(送信側)
ランダムチャレンジを生成する
S1
ランダムチャレンジを送信する
S2
N個の認証データの
期待値を生成する
S3
RC受信メッセージを受信する
S4
カウンタi←1
S5
コマンドを送信する
S6
応答時間計測を開始する
S7
応答メッセージを受信する
S8
応答時間計測を終了する
S9
認証データ＝期待値？
S10
NO
YES
YES
応答時間<=X？
S11
NO
i←i+1
S12
NO
i=N+1？
S13
YES
送信許可
S15
送信不許可
S14
判定終了メッセージを送信する
S16
エンド
応答処理スタート
(受信側)
S21
ランダムチャレンジを受信する
S22
N個の認証データを
生成する
S23
RC受信メッセージを送信する
S24
カウンタj←1
S25
認証データを含む
応答メッセージを生成する
S26
コマンドを受信する
S27
応答メッセージを送信する
S28
YES
判定終了メッセージが
受信されたか？
NO
j←j+1
S29
j=N+1？
S30
NO
YES
エンド

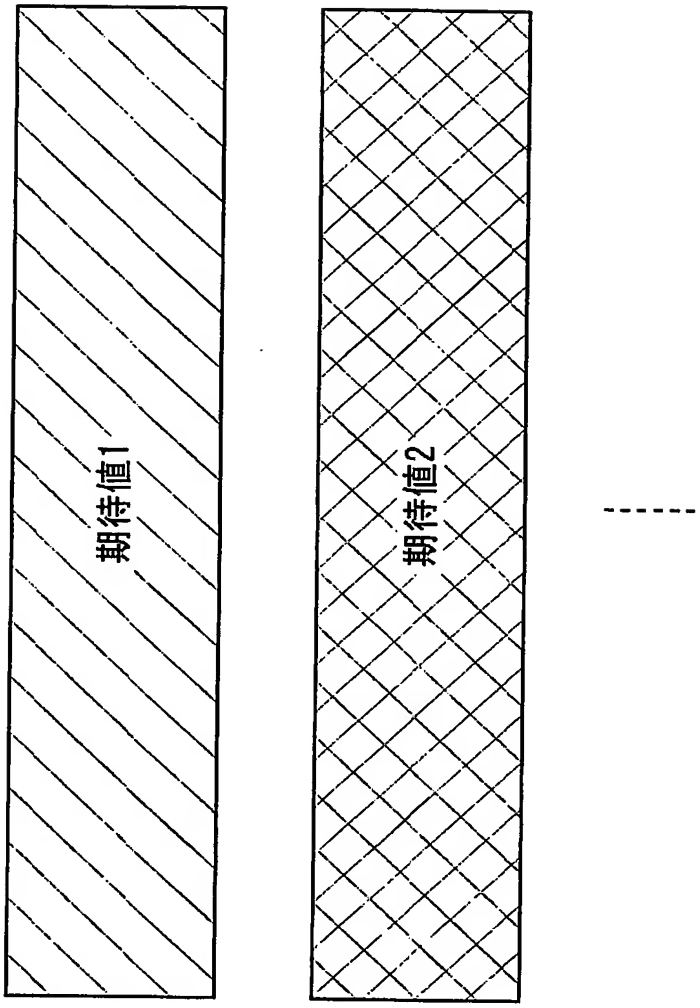
【図６】

図6



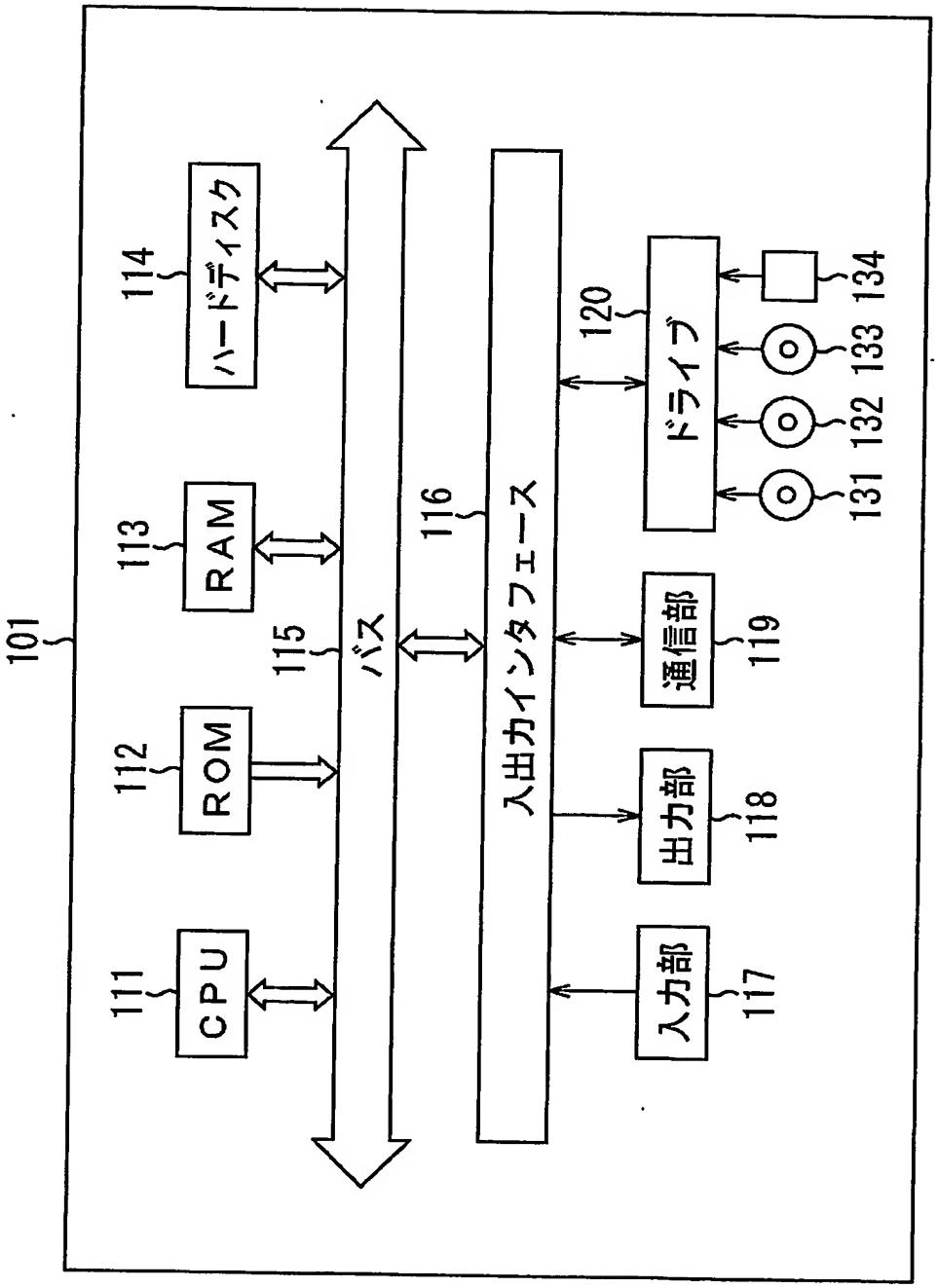
【図７】

図7



【図８】

図8


101
CPU
111
ROM
112
RAM
113
ハードディスク
114
バス
115
入出力インタフェース
116
入力部
117
出力部
118
通信部
119
ドライブ
120
131
132
133
134

【書類名】要約書
【要約】
【課題】通信時間を適切に計測することができるようにする。
【解決手段】受信制御部４１は、送信側の端末１１から送信されてきたランダムチャレンジを受信し、生成部４２に供給する。受信制御部４１はまた、ランダムチャレンジを受信した旨を表すＲＣ受信メッセージを、送信側の端末１１に送信する。生成部４２は、供給されたランダムチャレンジに対して、送信側の端末１１における場合と同様のハッシュ処理を施し、その結果得られた認証データを生成部４３に供給する。送信制御部４４は、送信側の端末からの応答要求コマンドを受信する前のタイミングで、生成部４３を制御して、受信する応答要求コマンドに対応した認証データを含む応答メッセージを生成させるとともに、応答要求コマンドを受信したとき、予め生成したその応答メッセージを送信先の端末に送信する。本発明は、コンテンツ提供システムに適用することができる。
【選択図】図４

出　願　人　履　歴　情　報

識別番号　　[０００００２１８５]

１．変更年月日　　１９９０年　８月３０日
[変更理由]　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社